Predicting Module Lattice Reduction

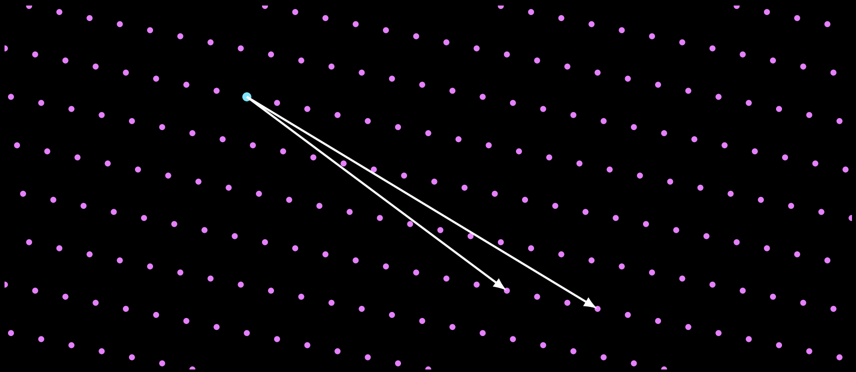
Full version: `https://eprint.iacr.org/2025/1904`
Accepted at Asiacrypt 2025

Paper by Léo Ducas[1,2], Lynn Engelberts[1,3] and **Paola de Perthuis**[1].

[1]: CWI, [2]: Leiden University, [3]: QuSoft

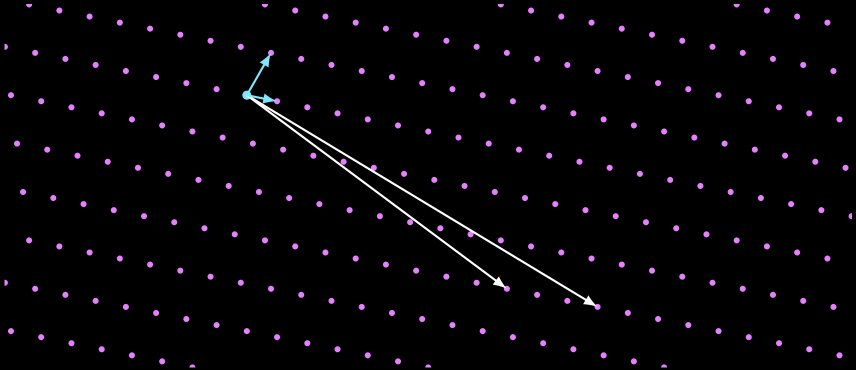
Introduction

Shortest Vector Problem



Introduction

Shortest Vector Problem



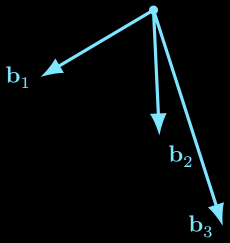
The BKZ Algorithm

Idea: consider β basis vectors at a time.

The BKZ Algorithm

Idea: consider β basis vectors at a time.

For each block:

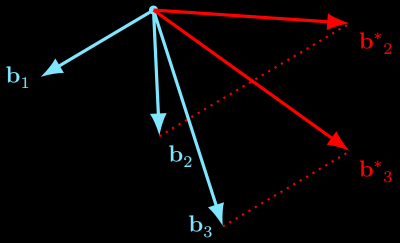


The BKZ Algorithm

Idea: consider β basis vectors at a time.

For each block:

1. project vectors orthogonally
   to those before the block



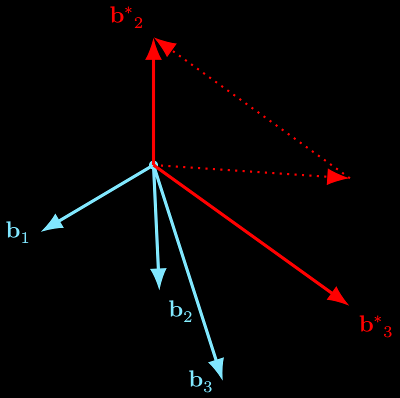
The BKZ Algorithm

Idea: consider β basis vectors at a time.

For each block:

1 project vectors orthogonally to those before the block

2 find shortest vector

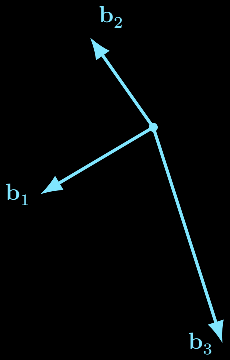


The BKZ Algorithm

Idea: consider β basis vectors at a time.

For each block:

1. project vectors orthogonally to those before the block
2. find shortest vector
3. lift back to the lattice

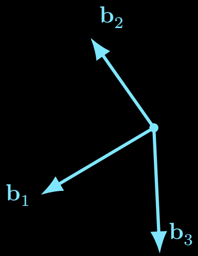


The BKZ Algorithm

Idea: consider β basis vectors at a time.

For each block:

1. project vectors orthogonally to those before the block
2. find shortest vector
3. lift back to the lattice
4. remove linear dependencies

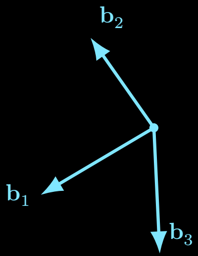


The BKZ Algorithm

Idea: consider β basis vectors at a time.

For each block:

1. project vectors orthogonally to those before the block
2. find shortest vector
3. lift back to the lattice
4. remove linear dependencies

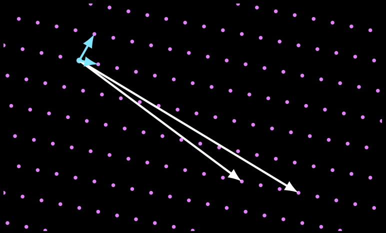


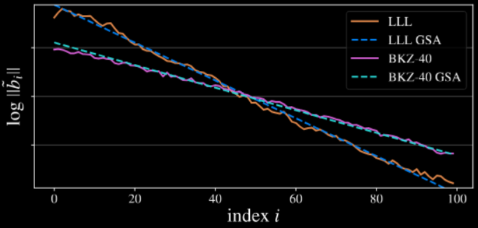
Uses Gram-Schmidt
linear orthogonal projections

The BKZ Algorithm

Cost: exponential in the blocksize β

Efficiency: better when flat orthogonalized basis profile





Example from [dBvW25]

Module Lattices

Number field $K = \mathbb{Q}[X]/P(X)$, where $P \in \mathbb{Q}[X]$ irreducible, of degree d.

$\mathcal{O}_K$ its ring of integers. $K_\mathbb{R} = K \otimes_\mathbb{Q} \mathbb{R}$

I fractional ideal of $\mathcal{O}_K$: $\mathcal{O}_K$-submodule of K s. t. $\exists x \in K^* \mid xI \subset \mathcal{O}_K$.

Module lattice M: defined with $\mathbf{b}_1, \dots, \mathbf{b}_r \in K_\mathbb{R}^\rho$ and $I_1, \dots, I_r$ fractional ideals of K, as $M = I_1\mathbf{b}_1 + \dots + I_r\mathbf{b}_r$.

Module Lattices

Number field $K = \mathbb{Q}[X]/P(X)$, where $P \in \mathbb{Q}[X]$ irreducible, of degree d.

$\mathcal{O}_K$ its ring of integers. $K_\mathbb{R} = K \otimes_\mathbb{Q} \mathbb{R}$

I fractional ideal of $\mathcal{O}_K$: $\mathcal{O}_K$-submodule of K s. t. $\exists x \in K^* \mid xI \subset \mathcal{O}_K$.

Module lattice M: defined with $\mathbf{b}_1, \ldots, \mathbf{b}_r \in K_\mathbb{R}^\rho$ and $I_1, \ldots, I_r$ fractional ideals of K, as $M = I_1\mathbf{b}_1 + \ldots + I_r\mathbf{b}_r$.

One may obtain a lattice in $\mathbb{R}^{d\rho}$ from M, by embedding elements of $K_\mathbb{R}$ into $\mathbb{R}^d$.

Ex.: canonical embedding, coefficient embedding.

mBKZ: BKZ Generalized to Modules (stemming from [LPSW19]'s mLLL)

Algorithm 1: mBKZ Algorithm Overview,
with an SVP oracle in dimension β_K

Input: pseudobasis $\mathcal{B} = (I_k, \mathbf{b}_k)_k$ of $M \subset K_{\mathbb{R}}^r$, blocksize β_K

while *this step changes* $\mathcal{B}$ **do**
  for i *in* $[\![1; r]\!]$ **do**
    $j \leftarrow \min(i + \beta_K - 1, r)$
    $\mathbf{v} \leftarrow \mathrm{SVP}\left(\pi_i\left(\mathcal{B}_{[\![i;j]\!]}\right)\right)$
    Let I be such that $\mathbf{v}I = \mathbf{v}K \cap \mathrm{Module}(\pi_i(\mathcal{B}_{[\![i;j]\!]}))$
    Let $\mathbf{w}$ be such that $\mathbf{w}I \subset M$ and $\pi_i(\mathbf{w}) = \mathbf{v}$
    Insert $(\mathbf{w}, I)$ into $\mathcal{B}$ at position i
    Remove linear dependencies

return $\mathcal{B}$

How does mBKZ perform with respect to BKZ?

How does mBKZ perform with respect to BKZ?

Can we do better than embedding M in $\mathbb{R}^{rd}$ and applying BKZ?

How does mBKZ perform with respect to BKZ?

Can we do better than embedding M in $\mathbb{R}^{rd}$ and applying BKZ?

Context of Post-Quantum Standardizations
$\rightarrow$ important to know whether the structure can be exploited

State-of-the-Art

[LPSW19, MS20]: defined module-lattice versions of lattice reduction, and studied their worst-case behavior only

[KK24]: first experimental study of module-LLL on NTRU lattices, results limited to LLL, power-of-two cyclotomics, and no predictive framework

Our contributions:
predictions for the average case, asymptotics, experiments.

Overview of the Presentation

A. The Geometric Series Assumption (GSA)

1. In the Unstructured Case (introduced in [Sch03])

For $(\mathbf{b}_1, \dots, \mathbf{b}_n) \in (\mathbb{R}^n)^n$ a lattice basis, ordered with vectors of descending norm, we denote $(\mathbf{b}_1^*, \dots, \mathbf{b}_n^*)$ its Gram-Schmidt orthogonalisation, obtained recursively by setting:

$$\mathbf{b}_1^* = \mathbf{b}_1 \text{ and, for each } i \in [\![2; n]\!]\text{: } \mathbf{b}_i^* = \pi_i(\mathbf{b}_i),$$

where $\pi_i^* : \mathbb{R}^n \to \mathbb{R}^n$ is the linear operation projecting vectors orthogonally to $\operatorname{span}_{\mathbb{R}}\{\mathbf{b}_1^*, \dots, \mathbf{b}_{i-1}^*\}$.

GSA Heuristic

Using an algorithm $\mathcal{A}$ to reduce a basis, there is an $\alpha_{\mathcal{A}} \in [0; 1]$ such that:

$$\forall i \in [\![1; n-1]\!], \left|\left|\mathbf{b}_{i+1}^*\right|\right| \approx \alpha_{\mathcal{A}} \left|\left|\mathbf{b}_i^*\right|\right|$$

A. The Geometric Series Assumption (GSA)

2. For Module BKZ

Norm and Determinant Notions:

Let $\sigma : K \to \mathbb{C}^d, x \mapsto (\sigma_1(x), \ldots, \sigma_d(x))$ denote the canonical embedding from K to $\mathbb{C}$.

Algebraic norm on $K_{\mathbb{R}}$ $\mathcal{N} : K_{\mathbb{R}} \to \mathbb{R}, x \mapsto \prod_i \sigma_i(x)$,
algebraic norm of a fractional ideal I of $\mathcal{O}_K$: $\mathcal{N}(I) = \frac{|\mathcal{O}_K / xI|}{\mathcal{N}(x)}$ for any $x \in K^* \mid xI \subset \mathcal{O}_K$.

$\langle \cdot, \cdot \rangle : K_{\mathbb{R}}^2 \to \mathbb{C}, (x, y) \mapsto \sum_i \sigma_i(x)\overline{\sigma_i(y)}$ defines the *trace* norm $||\cdot|| : K_{\mathbb{R}} \to \mathbb{R}, x \mapsto \sqrt{\langle x, x \rangle}$,
extended to $K_{\mathbb{R}}^r$ in the natural way (for Gram-Schmidt orthogonalisation).

Given $(\mathbf{b}_k, I_k)$ a pseudobasis of M, $B = (\mathbf{b}_k)_k$, we define:
$\det(M) = \sqrt{|\Delta_K|}^r \sqrt{\mathcal{N}\left(\det\left(\overline{B}^T B\right)\right)} \prod_k \mathcal{N}(I_k)$.

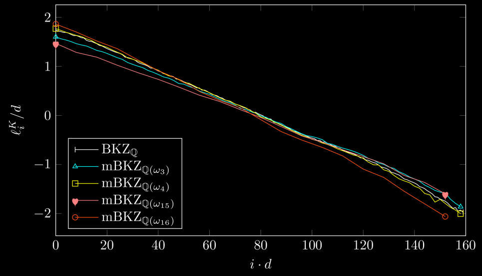
A. The Geometric Series Assumption (GSA)

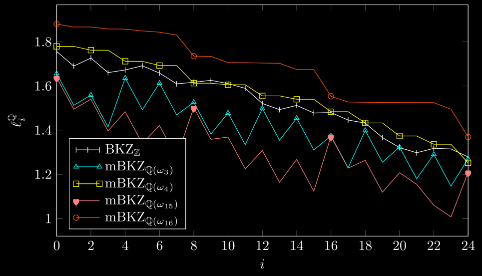
2. For Module BKZ

We Adapt the GSA Heuristic

For $(\mathbf{b}_k, I_k)_k$ a pseudobasis of $M \subset K_{\mathbb{R}}^r$ and $(\mathbf{b}_k^*)_k$ its Gram-Schmidt projection:

$$\forall k \in [\![1; r-1]\!]\,, \det(\mathbf{b}_k^* I_k) \approx \alpha \det(\mathbf{b}_{k-1}^* I_{k-1}).$$

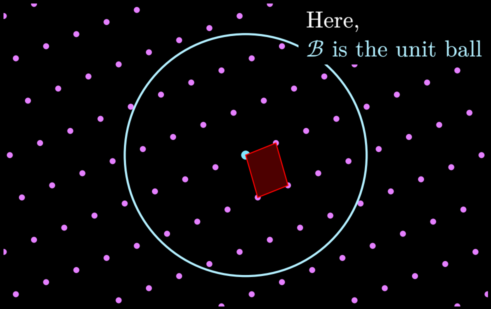




B. The Gaussian Heuristic

1. In the Unstructured Case

An example:



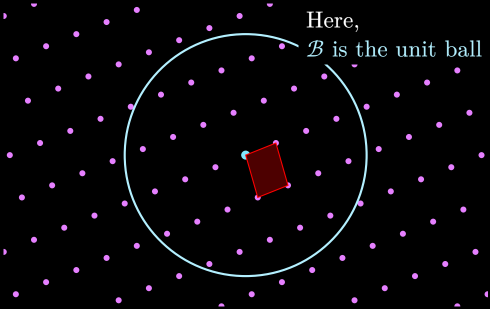
Here,
$\mathcal{B}$ is the unit ball

B. The Gaussian Heuristic

1. In the Unstructured Case

An example:

31 points inside $\mathcal{B}$, and $\frac{\mathrm{Vol}_{\mathcal{B}}}{\mathrm{Vol}_{\Lambda}} \approx 32$.



B. The Gaussian Heuristic

1. In the Unstructured Case

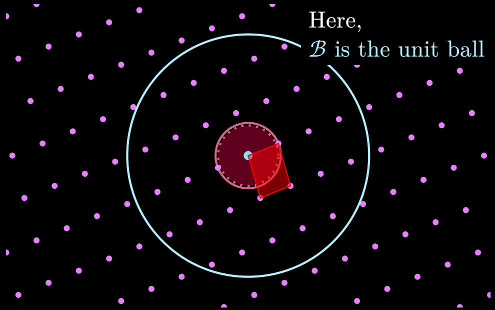
An example:

31 points inside $\mathcal{B}$, and $\frac{\mathrm{Vol}_{\mathcal{B}}}{\mathrm{Vol}_{\Lambda}} \approx 32$.

And approximation of shortest vector length as radius of ball with two points:

$$\lambda_1 \approx \left(\frac{2\mathrm{Vol}_{\Lambda}}{\mathrm{Vol}_{\mathcal{B}}}\right)^{\frac{1}{d}},$$

where d is the dimension.



B. The Gaussian Heuristic

1. In the Unstructured Case

An example:

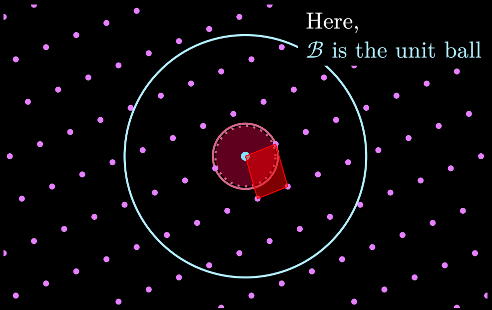
31 points inside $\mathcal{B}$, and $\frac{\mathrm{Vol}_{\mathcal{B}}}{\mathrm{Vol}_{\Lambda}} \approx 32$.

And approximation of shortest vector length as radius of ball with two points:

$$\lambda_1 \approx \left(\frac{2\mathrm{Vol}_{\Lambda}}{\mathrm{Vol}_{\mathcal{B}}}\right)^{\frac{1}{d}},$$

where d is the dimension.

Here: $\lambda_1 = 0.27 \approx 0.25$.



B. The Gaussian Heuristic

2. A Gaussian Heuristic for Modules (from [GSVV24])

The number field K of degree d's geometry yields new factor in λ_1 approximation for a module lattice $M \subset K_{\mathbb{R}}^r$.

Indeed, given a vector, other vectors of the same Euclidean norm will be provided by multiplication with roots of unity in K.
Hence the ball of radius λ_1 will hold $i \cdot \frac{\mu_K}{2} + 1$ points, for an integer i in $\mathbb{N}^*$ and μ_K the number of roots of unity in K. In our heuristics, we will consider that it will contain $\frac{\mu_K}{2} + 1$ points.

Overview of the Presentation

Expressing the Module-BKZ (mBKZ) Slope α_K

We Adapt the GSA Heuristic

We consider a distribution of random module lattices M of fixed determinant D such that, denoting $(\mathbf{b}_k, I_k)_k$ a pseudobasis of $M \subset K_{\mathbb{R}}^{\beta_K}$, and $(\mathbf{b}_k^*)_k$ its Gram-Schmidt orthogonalisation, generating the lattice M^*:

$$\forall k \in [\![1; \beta_K - 1]\!]\,, \mathbb{E}_M\{\ln(\det(\mathbf{b}_k^* I_k))\} = \ln(\alpha_K) + \mathbb{E}_M\{\ln\det(\mathbf{b}_{k-1}^* I_{k-1})\}.$$

Which yields, as $\det(\mathbf{b}_1^* I_1 + \cdots + \mathbf{b}_{\beta_K}^* I_{\beta_K}) = \det(M) = D$:

$$\frac{\beta_K(\beta_K - 1)}{2} \ln(\alpha_K) = \beta_K \mathbb{E}_M\{\ln\det(\mathbf{s}I)\} - \ln D,$$

where $\mathbf{s}$ is a shortest vector of Module(M^*) and I such that $\mathbf{s}I = \mathbf{s}K \cap M^*$
Expressing $\mathbb{E}_M\{\ln\det(\mathbf{s}I)\}$ provides the terms composing α_K.

Expressing the Module-BKZ (mBKZ) Slope α_K

We have $\frac{\beta_K - 1}{2} \ln(\alpha_K) = \mathbb{E}_M\{\ln \det(\mathrm{s}I)\} - \frac{\ln D}{\beta_K}$, where:

$$\mathbb{E}_M\{\ln \det(\mathrm{s}I)\} = \frac{1}{2}|\Delta_K| + \frac{1}{2}\mathbb{E}_M\left\{\ln \mathcal{N}\left(\bar{\mathrm{s}}^T \mathrm{s}\right)\right\} + \mathbb{E}_M\left\{\ln \mathcal{N}(I)\right\}.$$

So:

$$\boxed{\frac{\ln \alpha_K}{d} = \frac{2}{\beta_K - 1}\left(t_1 + t_2 + t_3 + t_4\right)}$$

Expressing the Module-BKZ (mBKZ) Slope α_K

We have $\frac{\beta_K - 1}{2} \ln(\alpha_K) = \mathbb{E}_M\{\ln \det(\mathrm{s}I)\} - \frac{\ln D}{\beta_K}$, where:

$$\mathbb{E}_M\{\ln \det(\mathrm{s}I)\} = \frac{1}{2}|\Delta_K| + \frac{1}{2}\mathbb{E}_M\left\{\ln \mathcal{N}\left(\bar{\mathrm{s}}^T \mathrm{s}\right)\right\} + \mathbb{E}_M\left\{\ln \mathcal{N}(I)\right\}.$$

So:

$$\boxed{\frac{\ln \alpha_K}{d} = \frac{2}{\beta_K - 1}\left(t_1 + t_2 + t_3 + t_4\right)}$$

where:

$$t_1 = \mathbb{E}_M\left\{\ln \frac{||\mathrm{s}||}{D^{\frac{1}{d\beta_K}}}\right\}$$

Expressing the Module-BKZ (mBKZ) Slope α_K

We have $\frac{\beta_K - 1}{2} \ln(\alpha_K) = \mathbb{E}_M\{\ln\det(\mathrm{s}I)\} - \frac{\ln D}{\beta_K}$, where:

$$\mathbb{E}_M\{\ln\det(\mathrm{s}I)\} = \frac{1}{2}|\Delta_K| + \frac{1}{2}\mathbb{E}_M\left\{\ln\mathcal{N}\left(\bar{\mathrm{s}}^T\mathrm{s}\right)\right\} + \mathbb{E}_M\left\{\ln\mathcal{N}(I)\right\}.$$

So:

$$\frac{\ln\alpha_K}{d} = \frac{2}{\beta_K - 1}\left(t_1 + t_2 + t_3 + t_4\right)$$

where:

$$t_1 = \mathbb{E}_M\left\{\ln\frac{||\mathrm{s}||}{D^{\frac{1}{d\beta_K}}}\right\} \qquad t_2 = \frac{1}{2d}\ln\frac{|\Delta_K|}{d^d}$$

Expressing the Module-BKZ (mBKZ) Slope α_K

We have $\frac{\beta_K - 1}{2} \ln(\alpha_K) = \mathbb{E}_M\{\ln\det(\mathrm{s}I)\} - \frac{\ln D}{\beta_K}$, where:

$$\mathbb{E}_M\{\ln\det(\mathrm{s}I)\} = \frac{1}{2}|\Delta_K| + \frac{1}{2}\mathbb{E}_M\left\{\ln\mathcal{N}\left(\bar{\mathrm{s}}^T\mathrm{s}\right)\right\} + \mathbb{E}_M\{\ln\mathcal{N}(I)\}.$$

So:

$$\frac{\ln\alpha_K}{d} = \frac{2}{\beta_K - 1}(t_1 + t_2 + t_3 + t_4)$$

where:

$$t_1 = \mathbb{E}_M\left\{\ln\frac{||\mathrm{s}||}{D^{\frac{1}{d\beta_K}}}\right\} \qquad t_2 = \frac{1}{2d}\ln\frac{|\Delta_K|}{d^d}$$

$$t_3 = \mathbb{E}_M\left\{\ln\frac{\sqrt{d}\mathcal{N}\left(\bar{\mathrm{s}}^T\mathrm{s}\right)^{\frac{1}{2d}}}{||\mathrm{s}||}\right\}$$

Expressing the Module-BKZ (mBKZ) Slope α_K

We have $\frac{\beta_K - 1}{2} \ln(\alpha_K) = \mathbb{E}_M\{\ln\det(\mathrm{s}I)\} - \frac{\ln D}{\beta_K}$, where:

$$\mathbb{E}_M\{\ln\det(\mathrm{s}I)\} = \frac{1}{2}|\Delta_K| + \frac{1}{2}\mathbb{E}_M\left\{\ln\mathcal{N}\left(\bar{\mathrm{s}}^T\mathrm{s}\right)\right\} + \mathbb{E}_M\{\ln\mathcal{N}(I)\}.$$

So:

$$\boxed{\frac{\ln\alpha_K}{d} = \frac{2}{\beta_K - 1}(t_1 + t_2 + t_3 + t_4)}$$

where:

$$t_1 = \mathbb{E}_M\left\{\ln\frac{||\mathrm{s}||}{D^{\frac{1}{d\beta_K}}}\right\} \qquad t_2 = \frac{1}{2d}\ln\frac{|\Delta_K|}{d^d}$$

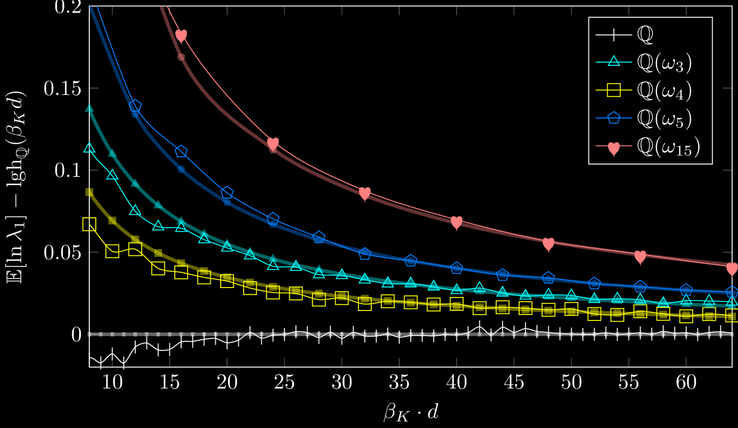
$$t_3 = \mathbb{E}_M\left\{\ln\frac{\sqrt{d}\mathcal{N}\left(\bar{\mathrm{s}}^T\mathrm{s}\right)^{\frac{1}{2d}}}{||\mathrm{s}||}\right\} \qquad t_4 = \frac{\mathbb{E}_M\{\ln\mathcal{N}(I)\}}{d}$$

The Gaussian Heuristic Term $t_1 = \mathbb{E}_M \left\{ \ln \frac{||\mathbf{s}||}{D^{\frac{1}{d\beta_K}}} \right\}$

The generalized Gaussian Heuristic for modules provides an estimation of t_1.

For K a field with μ_K roots of unity, denoting $\beta := d\beta_K$:

$t_1 \approx \frac{1}{\beta} \ln \left(\frac{\mu_K}{2\mathrm{Vol}(\mathcal{B}_\beta)} \right)$



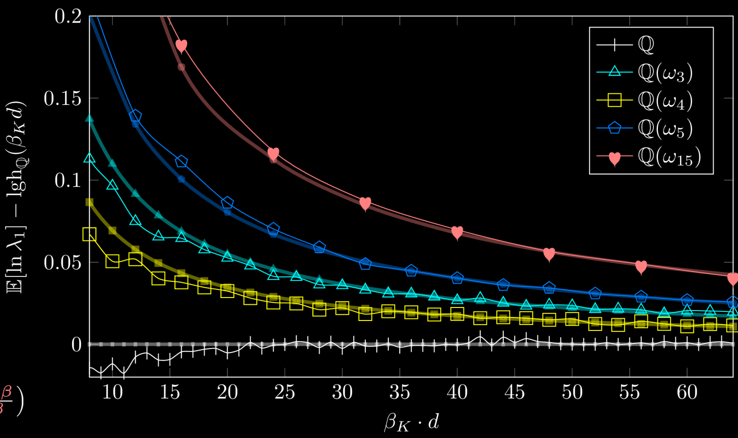
The Gaussian Heuristic Term $t_1 = \mathbb{E}_M \left\{ \ln \frac{||\mathbf{s}||}{D^{\frac{1}{d\beta_K}}} \right\}$

The generalized Gaussian Heuristic for modules provides an estimation of t_1.

For K a field with μ_K roots of unity, denoting $\beta := d\beta_K$:

$t_1 \approx \frac{1}{\beta} \ln \left(\frac{\mu_K}{2\mathrm{Vol}(\mathcal{B}_\beta)} \right)$

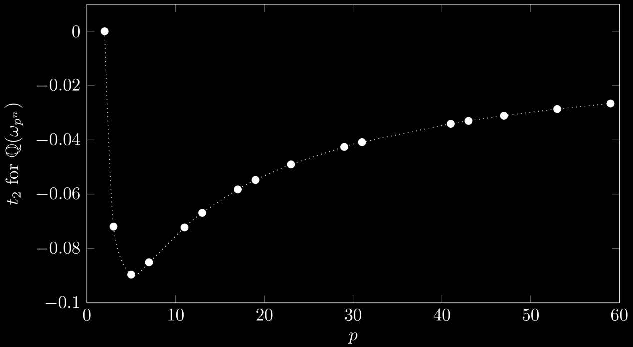
$= \frac{\ln(\beta+2)}{2} - \frac{\ln(2\pi e)}{2} + \frac{\ln \beta}{2\beta} + o\left(\frac{\ln \beta}{\beta}\right)$



The Discriminant Term $t_2 = \frac{1}{2d} \ln \frac{|\Delta_K|}{d^d}$

Constant in β_K.

We calculate this term for cyclotomic fields $K = \mathbb{Q}(\omega_c)$.

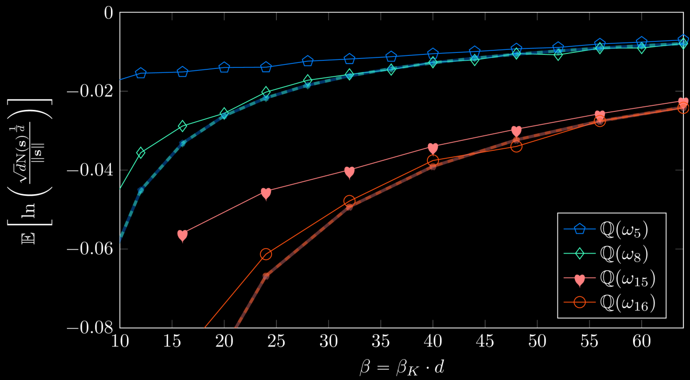


Then: $t_2 = \frac{1}{2} \sum_{\substack{p \mid c \\ p \text{ prime in } \mathbb{N}}} \left(\frac{p-2}{p-1} \ln(p) - \ln(p-1) \right).$

The Skewness Term $t_3 = \mathbb{E}_M\left\{ \ln \frac{\sqrt{d}\mathcal{N}\left(\bar{\mathbf{s}}^T\mathbf{s}\right)^{\frac{1}{2d}}}{||\mathbf{s}||} \right\}$

Using the canonical embedding, the arithmetico-geometric inequality gives $t_3 \leq 0$.

Then, modelling the shortest vector as uniform of a sphere yields, denoting ψ the digamma function, $(d_{\mathbb{R}}, d_{\mathbb{C}})$ the signature of K, and $\beta = d\beta_K$:

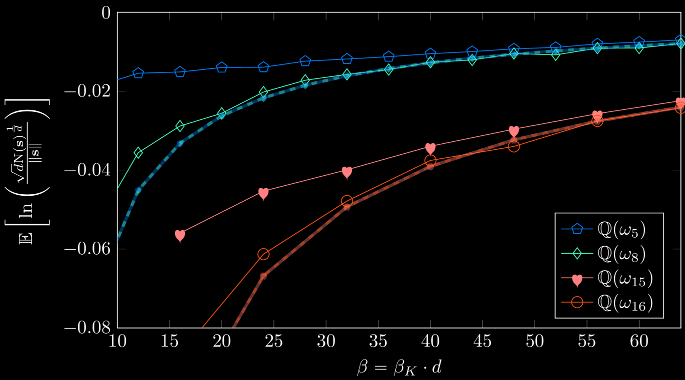


$$t_3 \approx \frac{1}{2}\left(\frac{d_{\mathbb{R}}\psi\left(\frac{\beta_K}{2}\right)+2d_{\mathbb{C}}(\psi(\beta_K)-\ln 2)}{d} + \ln d - \psi\left(\frac{\beta_K d}{2}\right)\right)$$

The Skewness Term $t_3 = \mathbb{E}_M\left\{ \ln \frac{\sqrt{d}\mathcal{N}\left(\bar{\mathbf{s}}^T\mathbf{s}\right)^{\frac{1}{2d}}}{||\mathbf{s}||} \right\}$

Using the canonical embedding, the arithmetico-geometric inequality gives $t_3 \leq 0$.

Then, modelling the shortest vector as uniform of a sphere yields, denoting ψ the digamma function, $(d_{\mathbb{R}}, d_{\mathbb{C}})$ the signature of K, and $\beta = d\beta_K$:

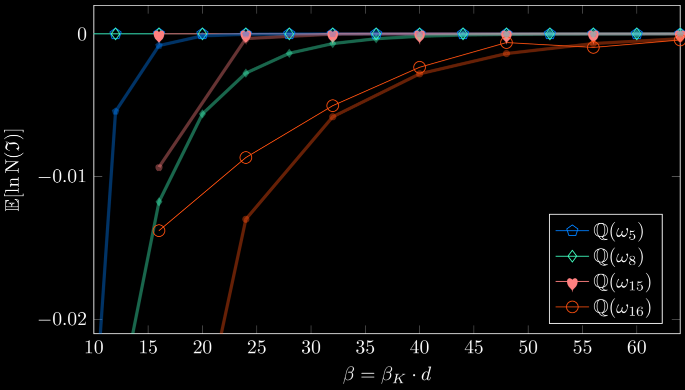


$$t_3 \approx \frac{1}{2}\left(\frac{d_{\mathbb{R}}\psi\left(\frac{\beta_K}{2}\right)+2d_{\mathbb{C}}(\psi(\beta_K)-\ln 2)}{d} + \ln d - \psi\left(\frac{\beta_K d}{2}\right)\right) = \frac{1-d_{\mathbb{R}}-d_{\mathbb{C}}}{2\beta} + o\left(\frac{1}{\beta}\right)$$

The Index Term $t_4 = \frac{\mathbb{E}_M\{\ln \mathcal{N}(I)\}}{d}$

The pseudobases are normalized to have $\mathcal{O}_K \subset I$,
so: $t_4 \leq 0$.

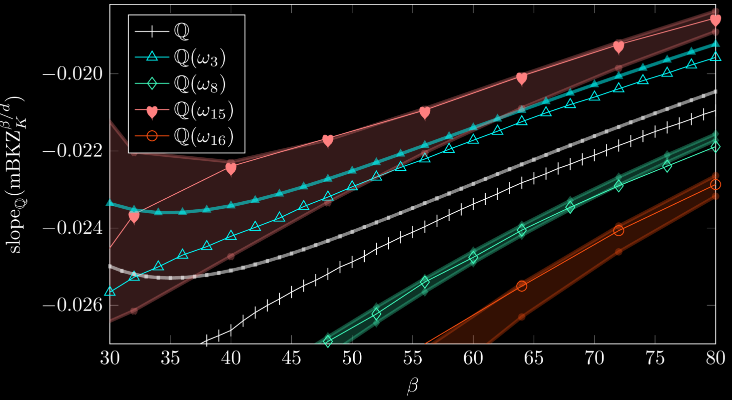
Modelling the probability that I^{-1} is a multiple of an ideal $\mathfrak{a} \subset \mathcal{O}_K$ as $\frac{1}{\mathcal{N}(\mathfrak{a})^{\beta_K}}$,
and denoting $\frac{\zeta_K'}{\zeta_K}$ the logarithmic derivative of the zeta function of K:



$$t_4 \gtrapprox \frac{1}{d}\frac{\zeta_K'(\beta_K)}{\zeta_K(\beta_K)} \geq -\frac{1}{2^{\beta_K - 1}} + o\left(\frac{1}{2^{\beta_K}}\right)$$

Comparing mBKZ and BKZ's Performances

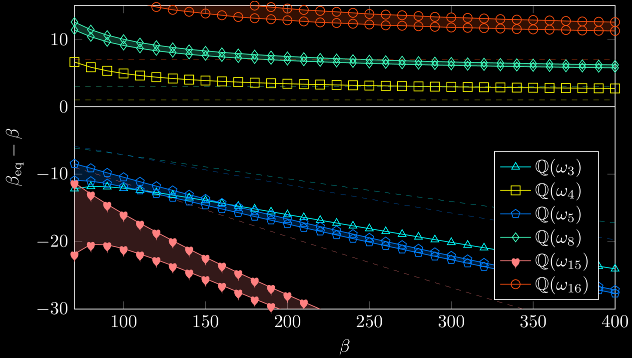
We implemented mBKZ and compare experimental slopes with our analysis bounding the $(t_i)_i$ terms. Implementation built on top of **pfLLL** and **g6k**.



Comparing mBKZ and BKZ's Performances

Denoting α the slope and β the block dimension in the unstructured case, $\frac{\ln \alpha_K}{d} = \alpha$, yields, denoting $\beta_{\text{eq}} = d\beta_K$:

$$\beta_{\text{eq}} = \beta + \log\left(\frac{|\Delta_K|}{d^d}\right)\frac{\beta}{d \ln \frac{\beta}{2\pi e}} + d - 1 + o(1)$$



Next Open Questions

1. HKZ profile, tails and dimensions for free
2. Simulation
3. Lattice sieving using cyclotomic symmetries
4. Coefficient embeddings
5. Algebraic-Norm SVP Oracle

Next Open Questions

1. HKZ profile, tails and dimensions for free
2. Simulation
3. Lattice sieving using cyclotomic symmetries
4. Coefficient embeddings
5. Algebraic-Norm SVP Oracle

Perthuis-Trenkić-2025:
Refined Modelling of the Primal Attack, and Variants Against Module-Learning With Errors,
ePrint 2025/2195

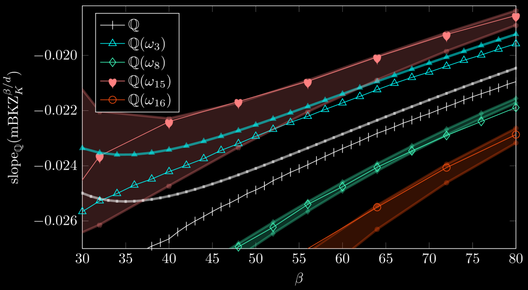
Next Open Questions

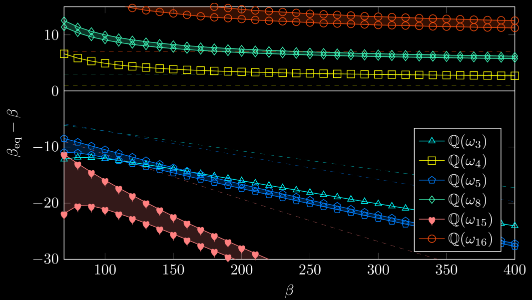
1. HKZ profile, tails and dimensions for free
2. Simulation
3. Lattice sieving using cyclotomic symmetries
4. Coefficient embeddings
5. Algebraic-Norm SVP Oracle

Perthuis-Trenkić-2025:
Refined Modelling of the Primal Attack, and Variants Against Module-Learning With Errors,
ePrint 2025/2195

Conclusion

Full version: `https://eprint.iacr.org/2025/1904`





Thank you for your attention!
Do you have questions?

Bibliography

[dBvW25] Koen de Boer and Wessel van Woerden. Lattice-based cryptography: A survey on the security of the lattice-based NIST finalists. Cryptology ePrint Archive, Paper 2025/304, 2025.

[GSVV24] Nihar Gargava, Vlad Serban, Maryna Viazovska, and Ilaria Viglino. Effective module lattices and their shortest vectors. 2024.

[KK24] Alexander Karenin and Elena Kirshanova. Finding dense submodules with algebraic lattice reduction. In Serge Vaudenay and Christophe Petit, editors, *AFRICACRYPT 24*, volume 14861 of *LNCS*, pages 403–427. Springer, Cham, July 2024.

[LPSW19] Changmin Lee, Alice Pellet-Mary, Damien Stehlé, and Alexandre Wallet. An LLL algorithm for module lattices. In Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT 2019, Part II*, volume 11922 of *LNCS*, pages 59–90. Springer, Cham, December 2019.

[MS20] Tamalika Mukherjee and Noah Stephens-Davidowitz. Lattice reduction for modules, or how to reduce ModuleSVP to ModuleSVP. In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part II*, volume 12171 of *LNCS*, pages 213–242. Springer, Cham, August 2020.

[Sch03] Claus-Peter Schnorr. Lattice reduction by random sampling and birthday methods. In *STACS 2003, 20th Annual Symposium on Theoretical Aspects of Computer Science, Berlin, Germany*, 2003.